

IN THE CLAIMS

Please cancel claims 1-38 without prejudice or disclaimer, and substitute new claims 39-77 therefor as follows:

Claims 1-38 (Cancelled).

39. (New) A method of providing intrusion detection in a network wherein data flows are exchanged using associated network ports and application layer protocols, comprising the steps of:

monitoring data flows in said network;

detecting information on said application layer protocols involved in said monitored data flows; and

providing intrusion detection on said monitored data flows based on application layer protocols detected.

40. (New) The method of claim 39, wherein said intrusion detection is provided independently of any predefined association between said network ports and said application layer protocols.

41. (New) The method of claim 39, wherein said step of detecting information on application layer protocols comprises passive observation of network traffic.

42. (New) The method of claim 39, wherein said step of detecting information on application layer protocols comprises using signature-matching techniques.

43. (New) The method of claim 39, wherein said step of detecting information on application layer protocols in said data flows comprises the step of identifying at least one protocol in a given data flow.

44. (New) The method of claim 39, wherein said step of providing intrusion detection comprises signature-based detection of misuse by matching at least one of a given data packet and data flow regardless of the service ports involved, based on said information on application layer protocols.

45. (New) The method of claim 39, comprising providing intrusion detection based on a plurality of predefined sets of analysis tasks and misuse signatures for a plurality of said protocols, and comprises selecting out of said plurality a set related to at least one protocol in a given data flow and at least one of the steps of:

performing over said data flow the selected set of analysis tasks; and

performing signature matching over said data flow against the selected set of misuse signatures.

46. (New) The method of claim 39, wherein said steps of detecting information on application layer protocols and providing intrusion detection are performed within the same functional module and employing the same functional blocks of packet capture, preprocessing and signature matching.

47. (New) The method of claims 42, wherein said signature-matching is performed by comparing monitored traffic with a set of protocol detection signatures having the following characteristics:

the set of signatures is specified in a language similar to the signature language used to specify misuse signatures in said network intrusion detection system, and

each said signature specifies a respective protocol that is detected if the signature is triggered.

48. (New) The method of claim 47, wherein each said signature is designed to attempt to match a pattern that is unique to a given protocol and at the same time is frequently used in said protocol.

49. (New) The method of claim 47, comprising the step of using at least one of the signatures identifying behavior frequently present in server responses and signatures identifying common client request-server reply behavior.

50. (New) The method of claim 47, comprising leaving out signatures exclusively matching a pattern in client behavior.

51. (New) The method of claim 39, wherein said step of detecting information on application layer protocols involved in said data flows comprises characterizing and classifying data flows related to each server application in said network.

52. (New) The method of claim 51, wherein said step of characterizing and classifying data flows comprises monitoring features from the group of: packet size, packet arrival times, TCP flags and header information.

53. (New) The method of claim 51, wherein said step of characterizing and classifying data flows comprises classifying data flows and services into a number of flow classes.

54. (New) The method of claim 51, wherein said step of characterizing and classifying data flows comprises at least one of discriminating between interactive and non-interactive traffic and identifying specific protocols.

55. (New) The method of claim 39, wherein said step of detecting information on application layer protocols in said data flows comprises producing a map of associations between application layer protocols and network ports present in said network, and said step of providing intrusion detection is performed on said associated network ports.

56. (New) The method of claim 39, wherein said step of providing intrusion detection based on said information on application layer protocols comprises the steps of:

- establishing a network policy, and
- generating a security event whenever a protocol is detected in violation of said network policy.

57. (New) A system for providing intrusion detection in a network wherein data flows are exchanged using associated network ports and application layer protocols, comprising:

- a monitoring module configured for monitoring data flows in said network;
- a protocol identification engine configured for detecting information on application layer protocols in said monitored data flows; and
- an intrusion detection module designed for operating on said monitored data flows based on said information on application layer protocols detected.

58. (New) The system of claim 57, wherein said intrusion detection module operates independently of any predefined association between said network ports and said application layer protocols.

59. (New) The system of claim 57, wherein said monitoring module is a module configured for passive observation of network traffic.

60. (New) The system of claim 59, wherein said module is a sniffer.

61. (New) The system of claim 57, wherein said protocol identification engine comprises a signature-matching feature.

62. (New) The system of claim 57, wherein said protocol identification engine is configured for detecting information on application layer protocols in said data flows by identifying at least one protocol in a given data flow.

63. (New) The system of claim 57, wherein said intrusion detection module is configured for providing intrusion detection by signature-based detection of misuse by matching at least one of a given data packet and data flow regardless of the service ports involved, based on said information on application layer protocols.

64. (New) The system of claim 57, wherein said intrusion detection module is configured for providing intrusion detection based on a plurality of predefined sets of analysis tasks and misuse signatures for a plurality of said protocols, said intrusion detection module being further configured for selecting out of said plurality a set related to at least one protocol in a given data flow and carrying out at least one of the steps of:

- performing over said data flow the selected set of analysis tasks, and
- performing signature matching over said data flow against the selected set of misuse signatures.

65. (New) The system of claim 57, wherein said protocol identification engine and said intrusion detection module are integrated to a common functional module and

employ a common set of functional blocks of packet capture, preprocessing and signature matching.

66. (New) The system of claim 61, comprising a configuration for performing said signature-matching by comparing monitored traffic with a set of protocol detection signatures having the following characteristics:

the set of signatures is specified in a language similar to the signature language used to specify misuse signatures in said network intrusion detection system, and

each said signature specifies a respective protocol that is detected if the signature is triggered.

67. (New) The system of claim 66, wherein each said signature is designed to attempt to match a pattern that is unique to a given protocol and at the same time is frequently used in said protocol.

68. (New) The system of claim 66, comprising a configuration for using at least one of the signatures identifying behavior frequently present in server responses and signatures identifying common client request-server reply behavior.

69. (New) The system of claim 66, comprising a configuration for leaving out signatures exclusively matching a pattern in client behavior.

70. (New) The system of claim 57, wherein said protocol identification engine is configured for detecting information on application layer protocols in said data flows by characterizing and classifying data flows related to each server application in said network.

71. (New) The system of claim 70, wherein said protocol identification engine is configured for monitoring features from the group of: packet size, packet arrival times, TCP flags and header information.

72. (New) The system of claim 70, wherein said protocol identification engine is configured for characterizing and classifying data flows by classifying data flows and services into a number of flow classes.

73. (New) The system of claim 70, wherein said protocol identification engine is configured for characterizing and classifying data by at least one of discriminating between interactive and non-interactive traffic and identifying specific protocols.

74. (New) The system of claim 58, wherein said protocol identification engine is configured for producing a map of associations between application layer protocols and network ports present in said network, and said intrusion detection module provides intrusion detection on said associated network ports.

75. (New) The system of claim 57, wherein said intrusion detection module is configured for:

establishing a network policy, and

generating a security event whenever a protocol is detected in violation of said network policy.

76. (New) A communication network comprising the system according to claim 57, associated therewith.

77. (New) A computer program product loadable in the memory of at least one computer and comprising software code portions capable of performing the steps of claim 39, when the product is run on a computer.